

Serial No. 09/929,142  
Docket No. YOR920010068US1  
YOR.270

**AMENDMENTS TO THE CLAIMS:**

**Please amend the claims as follows:**

1. (Currently Amended) A method of reducing warranty costs, comprising:
  - monitoring indicators in a computer system;
  - discriminating, by said computer system, between a hardware-induced problem or outage and a software-induced problem or outage in the computer system based on said indicators;
  - periodically storing said indicators prior to the problem or outage; and
  - automatically recovering from said software-induced problem or outage without any communication to a web site[[,]] and without a transmission of a recovery action to a user.
2. (Previously Presented) The method according to claim 1, wherein said indicators comprise indicators of system software and hardware health.
3. (Previously Presented) The method of claim 2, further comprising:
  - analyzing said indicators to determine whether the problem or outage was due to hardware or software, after the problem or outage occurs.
4. (Original) The method of claim 3, further comprising:
  - presenting information regarding a cause of the problem or outage to a user of the computer system to prevent an unnecessary service call and hardware replacement.

Serial No. 09/929,142  
Docket No. YOR920010068US1  
YOR.270

5. (Original) The method of claim 1, further comprising:

depending upon said determining of said hardware-induced problem or outage or said software-induced problem or outage, determining a manufacturer of said hardware or said software having undergone said problem or said outage.

6. (Previously Presented) The method of claim 1, wherein, in event of one of a hardware-induced problem or outage and a software-induced problem or outage, pre-outage data is stored in a log file across the outage.

7-14. (Canceled)

15. (Previously Presented) A method of reducing a trouble-shooting cost in a computer system, comprising:

sampling system health data from a plurality of sources, and storing said data in a log;

determining whether said outage event has occurred;

based on whether said outage event occurs, analyzing, by said computer, logged and other data to judge a likely cause of the event; and

if the outage event comprises a software outage or problem, determining whether automatic recovery is possible, and if so, invoking an automatic recovery mechanism and notifying a customer or field support personnel that said software outage or problem is the cause of the event, and identifying a faulty subsystem for subsequent troubleshooting,

Serial No. 09/929,142  
Docket No. YOR920010068US1  
YOR.270

wherein said automatic recovery mechanism is conducted without any of communication to a web site and user intervention.

16. (Canceled)

17. (Previously Presented) The method of claim 15, further comprising:

if the event the outage event comprises a software outage or problem, determining whether automatic recovery is possible, and if not, indicating that the event is due to said software outage or problem, and is not automatically recoverable, and notifying a customer or service technician to manually recover the fault.

18. (Previously Presented) The method of claim 15, further comprising:

determining whether the event comprises a software outage or problem and if not, determining whether a diagnosable hardware outage or problem exists.

19. (Previously Presented) The method of claim 18, further comprising:

if the event is judged to be caused by hardware, examining at least one of a hardware error log, an error register, and a hardware diagnostic, and attempting to localize a replaceable component that caused the event;

informing a customer or a service technician that the outage was due to hardware; and manually recovering the hardware by replacing only defective hardware.

Serial No. 09/929,142  
Docket No. YOR920010068US1  
YOR.270

20. (Previously Presented) A computer node associated with a computer system, comprising:

hardware for executing an operating system, at least one application program, and a system health monitoring program,

wherein said system health monitoring program gathers system software and hardware health data from an application program, an operating system, and the hardware, discriminates, without communication to a website or intervention by a user, a cause of an event comprising at least one of a problem or outage of said computer node, and periodically stores said system software and hardware health data prior to the event.

21. (Previously Presented) The computer node of claim 20, wherein said computer node comprises sources of information for assessing software and hardware health.

22. (Previously Presented) The computer node of claim 21, wherein said information is measured and logged prior to a failure event, and

wherein said system health monitoring program monitors at least one of resource consumption data, system and application software error logs, system utilization and performance data, and software error counts.

23. (Original) The computer node of claim 20, wherein said system health monitoring program monitors at least one of concurrent diagnostics, hardware error logs, and hardware error counts, and

Serial No. 09/929,142  
Docket No. YOR920010068US1  
YOR.270

wherein said system health monitoring program gathers information after the event, including at least one of error logs, crash dumps of memory, error codes, offline or power-on hardware diagnostics, and hardware error registers.

24. (Original) The computer node of claim 20, wherein said system health monitoring program includes a log device for permanently storing a time history of system software and hardware health data, said log device being readable after an event to determine a likely cause of the event.

25. (Original) The computer node of claim 20, wherein said system health monitoring program includes an analyzer for analyzing the software and hardware health data.

26. (Previously Presented) The computer node of claim 25, wherein said analyzer is run on one of the computer system that has experienced a problem, and another execution environment.

27. (Previously Presented) The computer node of claim 20, wherein said system health monitoring program comprises a notifier for notifying a customer or field service support personnel regarding a cause of the outage or problem, whether a service call is necessary, and where the likely cause of the outage or problem resides.

Serial No. 09/929,142  
Docket No. YOR920010068US1  
YOR.270

28. (Original) The computer node of claim 20, wherein said system health monitoring program samples a plurality of parameters, said plurality of parameters including at least one of:

a parameter indicating a number of bytes that must be kept in physical memory and cannot be paged out to disk;

a parameter indicating a number of bytes that reside in said physical memory plus the paging files;

a parameter indicating a number of errors that have been reported by transmission control protocol (TCP)/Internet Protocol (IP) software; and

a parameter indicating whether said TCP errors are accompanied by Network Adapter Errors.

29. (Previously Presented) A system for use with a computer system, comprising:

a software program for monitoring indicators in a computer;

an outage detector for detecting a problem or outage;

a memory for periodically storing said indicators prior to the problem or outage; and

a discriminator for discriminating, without any communication to a website or intervention by a user, whether said problem or outage was caused by a hardware component or a software component of said system.

30. (Previously Presented) The system according to claim 29, wherein, in event of an outage of one of said hardware and software, said indicators stored prior to the problem or outage are stored across the outage.

Serial No. 09/929,142  
Docket No. YOR920010068US1  
YOR.270

31. (Canceled)

32. (Previously Presented) The method according to claim 1, wherein said indicators comprise indicators of said software health comprising at least one of resource consumption data, system and application error logs, system utilization and preference data, and software error accounts.

33. (Previously Presented) The method according to claim 1, wherein said indicators comprise indicators of said hardware health comprising at least one of concurrent diagnostics, hardware error logs, and hardware error counts.

34. (Previously Presented) The method according to claim 1, further comprising:  
continuously monitoring and storing indicators of system software health and hardware health after said problem or outage.

35. (Previously Presented) The method according to claim 34, wherein said indicators monitored after said problem or outage comprise at least one of error logs, crash dumps or memory, error codes, offline or power-on hardware diagnostics and hardware error registers.

36. (Previously Presented) The method according to claim 1, wherein said monitoring comprises:

Serial No. 09/929,142  
Docket No. YOR920010068US1  
YOR.270

sampling a plurality of parameters comprising at least one of:

a parameter indicating a number of bytes that must be kept in physical memory and cannot be paged out to disk;

a parameter indicating a number of bytes that reside in said physical memory plus the paging files;

a parameter indicating a number of errors that have been reported by transmission control protocol (TCP)/Internet Protocol (IP) software; and

a parameter indicating whether said TCP errors are accompanied by Network Adapter Errors.

37. (Previously Presented) The method according to claim 1, wherein another execution environment is used to perform said monitoring.

38. (Previously Presented) The method according to claim 1, wherein said monitoring indicators in said computer system comprises monitoring said indicators prior to said problem or outage.

39-40. (Canceled)

41. (Previously Presented) The method according to claim 1, wherein said indicators comprise:



Serial No. 09/929,142  
Docket No. YOR920010068US1  
YOR.270

indicators of said software health comprising at least one of resource consumption data, system and application error logs, system utilization and preference data, and software error accounts;

indicators of said hardware health comprising at least one of concurrent diagnostics, hardware error logs, and hardware error counts, and

wherein sampling a plurality of parameters comprises at least one of:

a parameter indicating a number of bytes that must be kept in physical memory and cannot be paged out to disk;

a parameter indicating a number of bytes that reside in said physical memory and the paging files;

a parameter indicating a number of errors that have been reported by transmission control protocol (TCP)/Internet Protocol (IP) software; and

a parameter indicating whether said TCP errors are accompanied by Network Adapter Errors.